****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **10/18/2024** | **Rachel Siminski** |  |

## Client



## Developer

Rachel Siminski

## Algorithm Cipher

AES-256 is the recommended algorithm cipher for Artemis Financial. AES, Advanced Encryption Standard, is the standard algorithm cipher due to its high level of security. AES is a symmetric cipher, meaning it uses the same key to encrypt and decrypt the data, which is appropriate for Artemis Financial’s needs as they are not transmitting sensitive data to external users.

## Certificate Generation

A screenshot of a computer

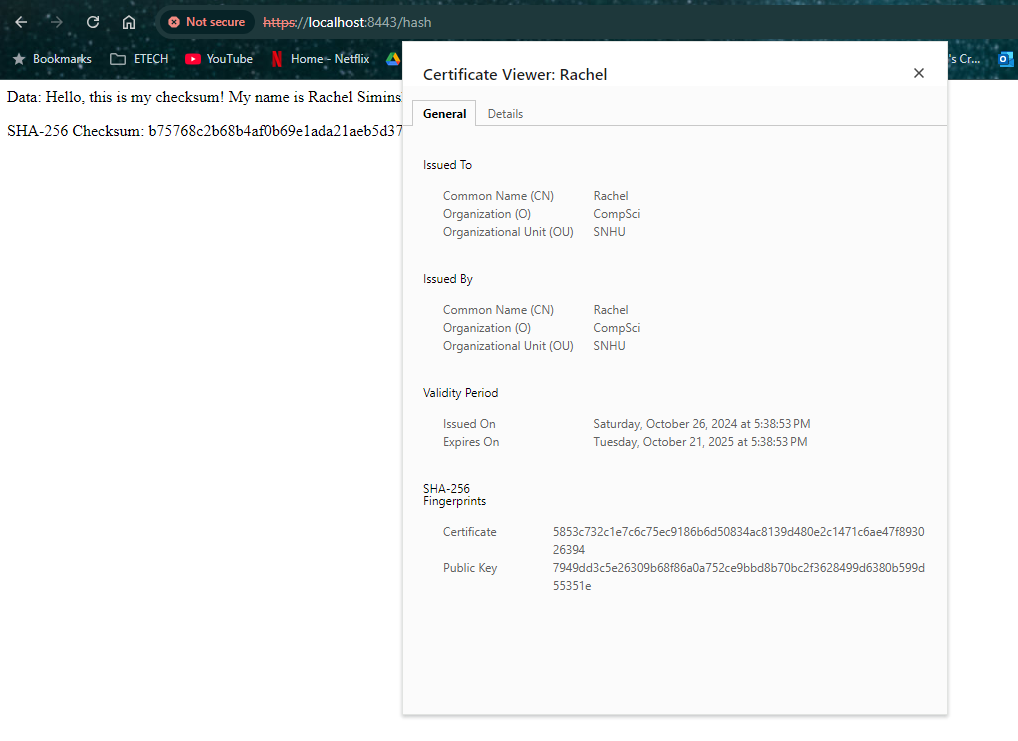
Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications



## Secondary Testing

A computer screen shot of text

Description automatically generatedA close-up of a text

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

## <file:///C:/Users/rache/HOMEWORK/Security/ssl-server_student/target/dependency-check-report.html>

## A screenshot of a computer Description automatically generated

## A screenshot of a computer Description automatically generated

## Summary

Based on the structure and functionality of the application false positive vulnerabilities were suppressed. Most of the vulnerabilities in the dependency check report were false positives, unrelated to anything in the program. The remaining vulnerabilities were relevant due to the application using HTTP and Spring Boot 2.2.4. To mitigate these vulnerabilities, I disabled the use of HTTP and enabled only HTTPS, and upgraded Spring Boot to 2.5.0, which automatically upgraded the Tomcat version from 9.0.34 to version 9.0.48. Once this was addressed the remaining false positives were suppressed.